Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

- Implement multifactor authentication (MFA) for all users.
- Enforce unique passwords for each employee.
- Remove the default admin account and assign a strong, unique password to admin roles.
- Configure firewalls with rules that block unauthorized incoming and outgoing traffic.

Part 2: Explain your recommendations

Implementing these controls will significantly reduce the risk of another data breach. MFA and strong password policies ensure that accounts cannot be easily accessed, even if credentials are leaked. Removing default credentials eliminates a common entry point for attackers. Firewall rules prevent suspicious traffic from entering or leaving the network. Together, these steps protect personal identifiable information (PII), help maintain customer trust, and reduce reputational and financial damage to the business.